PCT/DE 00/00827

BUNDESREPUBLIK DEUTSCHLAND

DE00/00827

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

EU 09/936291

REC'D 08 JUN 2000
WIPO PCT

Bescheinigung

Die Siemens Aktiengesellschaft in München/Deutschland hat eine Patentanmeldung unter der Bezeichnung

"Verfahren zur Prüfung der Authentität einer Manager Applikation in einem Telekommunikations Management Netz Bediensystem durch ein Netzelement sowie ein dafür geeignetes Netzelement"

am 19. März 1999 beim Deutschen Patent- und Markenamt eingereicht.

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

Die Anmeldung hat im Deutschen Patent- und Markenamt vorläufig das Symbol H 04 L 29/06 der Internationalen Patentklassifikation erhalten.

München, den 23. Mai 2000
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Aktenzeichen: 199 12 520.1

Ebert

A 9161
06.90
11/98

Beschreibung

Verfahren zur Prüfung der Authentität einer Manager Applikation in einem Telekommunikations Management Netz Bediensystem durch ein Netzelement sowie ein dafür geeignetes Netzelement

Die vorliegende Erfindung bezieht sich auf ein Verfahren zur Prüfung der Authentität einer Manager Applikation in einem Telekommunikations Management Netz Bediensystem (TMN-OS) gemäß dem Oberbegriff des Verfahrensanspruchs 1 und auf ein zugehöriges Netzelement gemäß dem Oberbegriff des Vorrichtungsanspruchs 5.

Vermittlungseinrichtungen, sog. Netzelemente, dienen als Knoten in einem Telekommunikationsnetz dazu, den Informationsfluß in solchen Netzen zu koordinieren. Die Netzelemente werden von einem speziellen Bediensystem, dem TMN-OS verwaltet. Zu diesem Zweck sind sie zusammen mit dem Bediensystem an ein spezielles Verwaltungsnetz, das sog. Telekommunikations Management Netz (TMN) angeschlossen; die Verwaltung der Netzelemente erfolgt durch Kommunikation des Bediensystems TMN-OS mit den Netzelementen über das TMN.

Das TMN-OS ist aus einer Vielzahl von Manager Applikationen aufgebaut, denen in jedem Netzelement jeweils ein Gegenpart, eine sog. Agent Applikation, zugeordnet ist.

Die Kommunikation zwischen einer Manager Applikation in dem TMN-OS und ihrer zugehörigen Agent Applikation in dem Netzelement erfolgt für jede Manager Applikation/Agent Applikation-Paarung gemäß einem fest definierten Kommunikationsprotokoll. Dabei wird zwischen "Veröffentlichten" und "Nicht-Veröffentlichten" Protokollen unterschieden. Veröffentlichte, sogenannte "Offene" Protokolle sind z.B. das FTAM-, das FTP- und das Q3-Protokoll. Im Gegensatz dazu ist z.B. das MML Protokoll, das "proprietär", also herstellerspezifisch definiert ist, nicht veröffentlicht.

Zu Beginn oder während der Abwicklung eines Kommunikationsprotokolles kann eine Prüfung der Authentität einer Manager Applikation durch ein Netzelement vorgesehen sein. Dazu muß sich die Manager Applikation, die eine Verbindung zu dem Netzelement aufzubauen wünscht, als diejenige ausweisen, die sie vorgibt zu sein.

Die Authentisierungsprüfung erfolgt in der Weise, daß die Manager Applikation kommunikationsprotokollspezifische Authentisierungsdaten über das TMN an das Netzelement überträgt, woraufhin das Netzelement die empfangenen Authentisierungsdaten mit vorbestimmten gespeicherten Authentisierungsdaten vergleicht.

Die Authentisierungsprüfung gestaltet sich insofern sehr kompliziert, da jedes Kommunikationsprotokoll nicht nur eine eigene Authentisierungsprüfung, sondern auch individuelle protokollspezifische Authentisierungsdaten besitzt. Als Authentitätsdaten dienen verschiedene Arten von Initiatoren und andere Daten. Zu den Initiatoren zählen z. B. Human-User, User Ids sowie Applikationen, die durch einen Application Entity Title (AET) gekennzeichnet sind. Andere Daten sind: Paßwörter, Schlüssel, Replay Protected Paßwörter, Randoms (Zufallszahlen), Datum und Uhrzeit etc.

Neben diesen unterschiedlichen protokollspezifischen Authentisierungsdaten stehen gemäß Fig. 2 für jedes Kommunikationsprotokoll i.d.R. mehrere Prüfmechanismen, sog. Authentisierungsarten, zur Durchführung der Authentisierungsprüfung zur Verfügung; gemäß Fig. 2 sind dies für das Kommunikationsprotokoll Q3 beispielsweise ein Simple Paßwort Mechanismus, ein Replay Protected Paßwort Mechanismus, eine reine "Identifizierung" oder ein Challenge & Response Verfahren.

Dies hat zur Folge, daß vor jeder Authentisierungsprüfung eine der jeweils zur Verfügung stehenden Authentisierungsarten

zur Durchführung der anstehenden Authentisierungsprüfung ausgewählt werden muß.

Herkömmlicherweise existieren deshalb für jedes Kommunikationsprotokoll unterschiedliche Softwareprogramme, sog. protokollspezifische Applikationen, mit teilweise sogar unterschiedlichen Bedieneroberflächen (MML, Q3) für die Verwaltung der Authentisierungsdaten und der Authentisierungsarten.

Es ist die Aufgabe der Erfindung, ein gegenüber dem herkömmlichen vereinfachtes Verfahren zur Prüfung der Authentität einer Manager Applikation durch ein Netzelement sowie ein dafür geeignetes Netzelement bereit zu stellen, bei denen die unterschiedlichen protokollspezifischen Applikationen zur Verwaltung der Authentisierungsdaten entbehrlich sind.

Diese Aufgabe wird durch die in den Patentansprüchen 1 und 5 beanspruchten Gegenstände gelöst. Weitere vorteilhafte Ausgestaltungen der Erfindung sind Gegenstand der Unteransprüche.

Gemäß den Patentansprüchen 1 und 5 wird die Aufgabe insbesondere dadurch gelöst, daß die Authentisierungsprüfung in dem Netzelement für verschiedene Manager Applikationen, das heißt für verschiedene Kommunikationsprotokolle, zentral in einer Authentisierungssprüfeinrichtung erfolgt, und daß die Authentisierungssprüfeinrichtung auf eine Authentisierungsdatenbank zugreift, in der die unterschiedlichen Authentisierungsdaten für alle verwendeten Kommunikationsprotokolle zentral hinterlegt sind.

Das erfindungsgemäße Verfahren sowie das dazugehörige Netzelement bieten den Vorteil, daß die Authentisierungsprüfung zentral und einheitlich für alle Kommunikationsprotokolle durchgeführt werden kann. Die Durchführung kommunikationsprotokollspezifischer Authentisierungsprüfungen wird damit entbehrlich.

Weiterhin wird durch die zentrale Authentisierungsdatenbank die Verwaltung der unterschiedlichen Authentisierungsdaten erheblich vereinfacht und verbilligt. Unterschiedliche Applikationen zur Verwaltung der kommunikationsprotokollspezifischen Authentisierungsdaten werden ebenfalls entbehrlich.

Außerdem lassen sich die zentrale Authentitätsprüfeinrichtung sowie die zentrale Authentisierungsdatenbank einfach ändern oder erweitern, wenn andere oder zusätzliche Kommunikationsprotokolle eingesetzt werden.

Gemäß einer vorteilhaften Ausgestaltung des Verfahrens wird die zentrale Authentisierungsdatenbank durch ein eigenes Kommunikationsprotokoll verwaltet. Auf diese Weise wird die Verwaltung der unterschiedlichen Authentisierungsdaten der verschiedenen Kommunikationsprotokolle vereinheitlicht, in dem z. B. eine einheitliche Bedieneroberfläche (MML, Q3) für die Verwaltung der unterschiedlichen Authentisierungsdaten realisiert wird.

Es ist von Vorteil, wenn für die Kommunikation zwischen den Manager Applikationen in dem TMN-OS und den Agent Applikationen in dem Netzelement verschiedene Kommunikationsprotokolle für den Austausch unterschiedlicher Informationen zur Verfügung stehen.

In einer bevorzugten Weiterbildung des erfindungsgemäßen Prüfungsverfahrens wird der Schritt der Authentisierungsprüfung nicht nur für jedes einzelnen Kommunikationsprotokoll, sondern auch für unterschiedliche Authentisierungsarten zentral in dem Netzelement durchgeführt. Auch diese Zentralisierung erspart kostenaufwendige kommunikationsprotokollspezifische Einzellösungen.

Schließlich ist es bei dem zur Durchführung des Verfahrens ausgebildeten Netzelement von Vorteil, wenn die zentrale Authentisierungsdatenbank von einer Verwaltungseinrichtung ver-

waltet wird, die über eine eigene netzelementinterne Agent Applikation von dem TMN-OS gesteuert wird. Neben der Einsparung von kommunikationsprotokollspezifischen Einzellösungen zur Verwaltung der kommunikationsprotokollspezifischen Authentisierungsdaten ermöglicht diese Weiterbildung außerdem eine Entkopplung von telekommunikationsspezifischer und verwaltungstechnischer Kommunikation zwischen dem TMN-OS und dem Netzelement.

Es erfolgt eine detaillierte Beschreibung eines bevorzugten Ausführungsbeispiels der Erfindung unter Bezugnahme auf die beigefügten Figuren.

Fig. 1 zeigt ein TMN als Verbindungsnetz zwischen einem TMN-OS und einem Netzelement gemäß der vorliegenden Erfindung; und

Fig. 2 zeigt eine tabellarische Zuordnung von Kommunikationsprotokollen und jeweils möglichen Authentisierungsarten.

Ein Netzelement in einem Kommunikationsnetz wird durch ein Telekommunikations Management Netz Bediensystem (TMN-OS) verwaltet. Fig. 1 zeigt die zu diesem Zweck erforderliche Ankopplung des Netzelementes an das TMN-OS über ein TMN. Das TMN-OS weist eine Vielzahl von Manager Applikationen 50, 60...100 auf, die entweder in Hardware, üblicherweise jedoch in Software realisiert werden. Ein oder mehrere dieser Manager Applikationen können dann auf einem Rechner ablaufen.

Das Netzelement weist zu jeder Manager Applikation in dem TMN-OS jeweils einen entsprechenden Gegenpart, eine sog. Agent Applikation 55, 65...105, auf. Über diese Agent Applikationen kommuniziert das Netzelement über das TMN mit den Manager Applikationen 50, 60...100 des TMN-OS. Jede Manager Applikation kommuniziert mit ihrer zugehörigen Agent Applikation in Form eines individuellen Kommunikationsprotokolls. Dabei sind gemäß Fig. 1 folgende Konstellationen möglich:

Die File Transfer Access Management (FTAM)-Manager Applikation 50 kommuniziert mit der FTAM-Agent Applikation 55;

die File Transfer Protocol (FTP)-Manager Applikation 60 kommuniziert mit der FTP-Agent Applikation 65;

die Man Machine Language (MML)-Manager Applikation 70 kommuniziert mit der MML-Agent-Applikation 75; und

die Q3-Manager Applikationen 80, 100 kommunizieren mit den Q3-Agent Applikationen 85, 105 in dem Netzelement.

Es wird eine unilaterale Authentisierungsprüfung betrachtet, bei der das Netzelement vor einem Verbindungsaufbau zu dem TMN-OS überprüft, ob die Manager Applikation, die eine Verbindung aufzubauen wünscht, diejenige ist, die sie vorgibt zu sein. Die Authentisierungsprüfung kann nicht nur vor, sondern auch während der Abwicklung eines Kommunikationsprotokolls, dann als eine sog. Re-Authentisierung, durchgeführt werden.

Im Rahmen der in Fig. 1 gezeigten unilateralen Authentisierungsprüfung baut eine Manager Applikation 50, 60...100, die eine Verbindung zu dem Netzelement aufbauen möchte, zunächst in Abhängigkeit ihres Kommunikationsprotokolles, ihrer Initiatoren und einer ausgewählten Authentisierungsart die für die Durchführung der Authentisierungsprüfung notwendigen Protokollanteile auf und sendet diese an das Netzelement. Von dem Netzelement werden diese Protokollanteile empfangen und ausgewertet. Bei der Auswertung werden insbesondere die für die Durchführung der Authentisierungsprüfung notwendigen Authentisierungsdaten aus den Protokollanteilen herausgefiltert.

Jedes der verwendeten Kommunikationsprotokolle, z. B. das FTAM-, das FTP-, das MML- oder das Q3-Kommunikationsprotokoll, besitzt jeweils eigene Authentisierungsdaten.

Als Authentisierungsdaten dienen verschiedene Arten von Initiatoren und andere Daten. Zu den Initiatoren zählen z. B. Human-User, User Ids sowie Applikationen, die durch einen Application Entity Title (AET) gekennzeichnet sind. Andere Daten sind: Paßwörter, Schlüssel, Replay Protected Paßwörter, Randoms (Zufallszahlen), Datum oder Uhrzeit etc.

Die von den Agent Applikationen 55, 65...105 selektierten Authentisierungsdaten werden innerhalb des Netzelementes an eine zentrale Authentisierungsprüfeinrichtung 20 weitergeleitet, wo sie zur Durchführung der eigentlichen Authentisierungsprüfung dienen.

Für jede Manager Applikation bzw. für jedes Kommunikationsprotokoll stehen gemäß Fig. 2 mehrere Mechanismen, sog. Authentisierungsarten, für die Durchführung einer Authentisierungsprüfung zur Verfügung. Für jede Authentisierungsprüfung wird im Einzelfall eine der möglichen Authentisierungsarten ausgewählt und vorbestimmt.

Die Authentisierungsprüfung erfolgt in der Weise, daß die zentrale Authentisierungsprüfeinrichtung 20 überprüft, ob die von der Manager Applikation gewünschte Authentisierungsart für das Kommunikationsprotokoll bzw. für den Initiator gültig ist, und ob die empfangenen protokollspezifischen Authentisierungsdaten mit den vorab in einer zentralen Authentisierungsdatenbank 10 hinterlegten originalen Authentisierungsdaten übereinstimmen. Im Falle einer Übereinstimmung stellt die zentrale Authentisierungsprüfeinrichtung fest, daß die anfragende Manager Applikation für einen beantragten Verbindungsaufbau berechtigt ist. Dazu folgendes Beispiel:

Im Vorfeld zukünftiger Kommunikationen zwischen dem TMN-OS und dem Netzelement werden zunächst Authentisierungsdaten für ein zu verwendendes Protokoll in der zentralen Authentisierungsdatenbank 10 hinterlegt. Dies erfolgt in der Weise, daß

eine Q3-Manager Applikation eine Q3-Verwaltungseinrichtung 30 innerhalb des Netzelementes beauftragt, in die zentrale Authentisierungsdatenbank 10 z. B. für zukünftige Kommunikationen mit dem FTAM-Protokoll den Initiator "HUGO" einzutragen, sowie daß dieser zur Authentisierung die Authentisierungsart "Simple Paßwort Mechanismus" benutzen muß und daß sein Kennwort "ABCD1#" ist.

Vor jedem nachfolgenden Verbindungsaufbau mit einem FTAM-Kommunikationsprotokoll führt dann die zentrale Authentisierungsprüfeinrichtung 20 im Netzelement die Authentisierungsprüfung wie folgt durch:

Von der FTAM-Agent Applikation 55 im Netzelement erhält sie die Information, daß die FTAM-Manager Applikation 50 eine Verbindung aufbauen möchte, wobei sich die Manager Applikation als Initiator "HUGO" der beantragten Verbindung ausgibt und behauptet, daß ihr Kennwort "ABCD1#" laute. Die zentrale Authentisierungsprüfeinrichtung 20 vergleicht daraufhin diese Daten mit den zuvor in der zentralen Authentisierungsdatenbank 10 hinterlegten originalen Authentisierungsdaten für das FTAM-Kommunikationsprotokoll und den Initiator "HUGO" und gibt im Falle einer Übereinstimmung den Verbindungsaufbau frei.

Am Ende einer Authentisierungsprüfung wird der Manager Applikation von ihrer zugehörigen Agent Applikation das Ergebnis ihrer Überprüfung zusammen mit den daraus resultierenden Konsequenzen für den Verbindungsaufbau mitgeteilt. Als mögliche Konsequenzen aus dem Ergebnis kommen folgende Entscheidungen in Frage: der beantragte Verbindungsaufbau erfolgt, der beantragte Verbindungsaufbau wird abgewiesen oder ein angefangener Verbindungsaufbau wird abgebrochen.

Die zentrale Authentisierungsprüfeinrichtung 20 führt die beispielhaft für das FTAM-Kommunikationsprotokoll beschriebene Authentisierungsprüfung in gleicher Weise für alle anderen

verwendeten Kommunikationsprotokolle durch. Sie greift dabei in jedem Einzelfall auf die zentrale Authentisierungsdatenbank 10 zu, in der die Authentisierungsdaten für alle Kommunikationsprotokolle hinterlegt sind.

Wie in Fig. 1 zu erkennen, wird die zentrale Authentisierungsdatenbank 10 von einer eigenen Q3-Manager Applikation 100 in dem TMN-OS verwaltet. Dabei läuft die Kommunikation der Q3-Manager Applikation 100 mit dem Netzelement ebenfalls über das TMN und eine zugehörige Q3-Agent Applikation 105. In dem Netzelement steuert die Q3-Agent Applikation 105 die Q3-Verwaltungseinrichtung 30, welche unmittelbar die zentrale Authentisierungsdatenbank 10 verwaltet. Typische Administrationsbefehle, die die Q3-Verwaltungseinrichtung 30 von der Q3-Manager Applikation 100 bzw. von ihrer zugehörigen Q3-Agent Applikation 105 erhält, sind z. B. das Eintragen, das Ändern oder das Löschen von Daten in der zentralen Authentisierungsdatenbank 10.

Neben der bisher diskutierten unilateralen Authentisierungsprüfung besteht grundsätzlich auch die Möglichkeit einer mutualen (oder gegenseitigen) Authentisierungsprüfung, die neben der beschriebenen unilateralen Authentisierungsprüfung auch die Prüfung der Authentität eines Netzelementes bzw. der Agent Application durch eine Manager Applikation vorsieht. Dabei muß sich die Agent Applikation, welche eine Kommunikation zu dem Bediensystem, bzw. zu einer Manager Applikation in dem Bediensystem aufzubauen wünscht, der Manager Applikation gegenüber als diejenige Agent Applikation ausweisen, welche sie vorgibt zu sein.

Patentansprüche

1. Verfahren zur Prüfung der Authentität einer Manager Applikation (50...100) in einem Telekommunikations Management Netz Bediensystem TMN-OS durch ein Netzelement, welches durch das TMN-OS über ein zwischengeschaltetes TMN verwaltet wird, mit folgenden Schritten:

Übertragen von kommunikationsprotokollspezifischen Authentisierungsdaten von einer Manager Applikation (50, 60...100) über das TMN an das Netzelement im Rahmen der Abwicklung eines Kommunikationsprotokolls, wobei die protokollspezifischen Authentisierungsdaten für die Prüfung der Authentität der Manager Applikation (50, 60...100) durch das Netzelement erforderlich sind; und

Überprüfen der Authentität der Manager Applikation durch Vergleichen der empfangenen protokollspezifischen Authentisierungsdaten mit vorbestimmten, gespeicherten Authentisierungsdaten;

dadurch gekennzeichnet, daß

der Schritt der Authentisierungsprüfung zentral in einer Authentitätsprüfeinrichtung (20) für verschiedene Kommunikationsprotokolle erfolgt; und daß

in einer Authentisierungsdatenbank (10) Authentisierungsdaten für alle verwendeten Kommunikationsprotokolle zentral hinterlegt sind.

2. Verfahren nach Anspruch 1, weiterhin gekennzeichnet durch folgenden Schritt:

Verwalten der zentralen Authentisierungsdatenbank (10) durch ein eigenes Kommunikationsprotokoll.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß das die Kommunikationsprotokolle ein Q3-, ein FTAM-, ein FTP- oder ein MML-Protokoll sind.

4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß der Schritt der Authentisierungsprüfung für jedes einzelne Kommunikationsprotokoll mit unterschiedlichen Authentisierungsarten zentral in der Authentitätsprüfeinrichtung (20) erfolgt.

5. Netzelement in einem Telekommunikationsnetz, wobei das Netzelement durch ein Telekommunikations Management Netz Bediensystem TMN-OS über ein Telekommunikations Management Netz TMN verwaltet wird, mit:

wenigstens einer Agent Applikation (55, 65...105) zum Empfangen von kommunikationsprotokollspezifischen Authentisierungsdaten über das TMN von einer zugehörigen Manager Applikation (50, 60...100) in dem TMN-OS, wobei die Authentisierungsdaten für die Prüfung der Authentität der zugehörigen Manager Applikation erforderlich sind; und

einer Authentitätsprüfeinrichtung (20), zum Empfangen der protokollspezifischen Authentisierungsdaten von der Agent Applikation und zum Prüfen der Authentität der Manager Applikation, durch Vergleichen der protokollspezifischen Authentisierungsdaten mit vorbestimmten, gespeicherten Authentisierungsdaten;

dadurch gekennzeichent, daß

die Authentitätsprüfeinrichtung (20) die Authentisierungsprüfung zentral für verschiedene Kommunikationsprotokolle durchführt, und daß

in einer Authentisierungsdatenbank (10) die Authentisierungsdaten für alle verwendeten Kommunikationsprotokolle zentral hinterlegt sind.

6. Netzelement nach Anspruch 5, dadurch gekennzeichnet, daß es weiterhin eine Verwaltungseinrichtung (30) umfaßt, welche die zentrale Authentisierungsdatenbank (10) verwaltet.

7. Netzelement nach Anspruch 6, dadurch gekennzeichnet, daß die Verwaltungseinrichtung (30) über eine eigene Agent Applikation (105) an das TMN angekoppelt ist und von dem TMN-OS gesteuert wird.

Zusammenfassung

Verfahren zur Prüfung der Authentität einer Manager Appliaktion in einem Telekommunikations Management Netz Bediensystem durch ein Netzelement sowie ein dafür geeignetes Netzelement

Die Verwaltung von Netzelementen in Telekommunikationsnetzen erfolgt über ein Bediensystem, das an die Netzelemente angeschlossen ist. Das Bediensystem ist aus einer Vielzahl von Manager Applikationen aufgebaut, die mit den Netzelementen kommunizieren. Im Rahmen einer solchen Kommunikation kann eine Authentisierungsprüfung einer Manager Applikation durch ein Netzelement vorgesehen sein. Erfindungsgemäß erfolgt diese Authentisierungsprüfung in dem Netzelement zentral für verschiedene Kommunikationsprotokolle, wobei auf eine zentrale Authentisierungsdatenbank 10 zugegriffen wird.

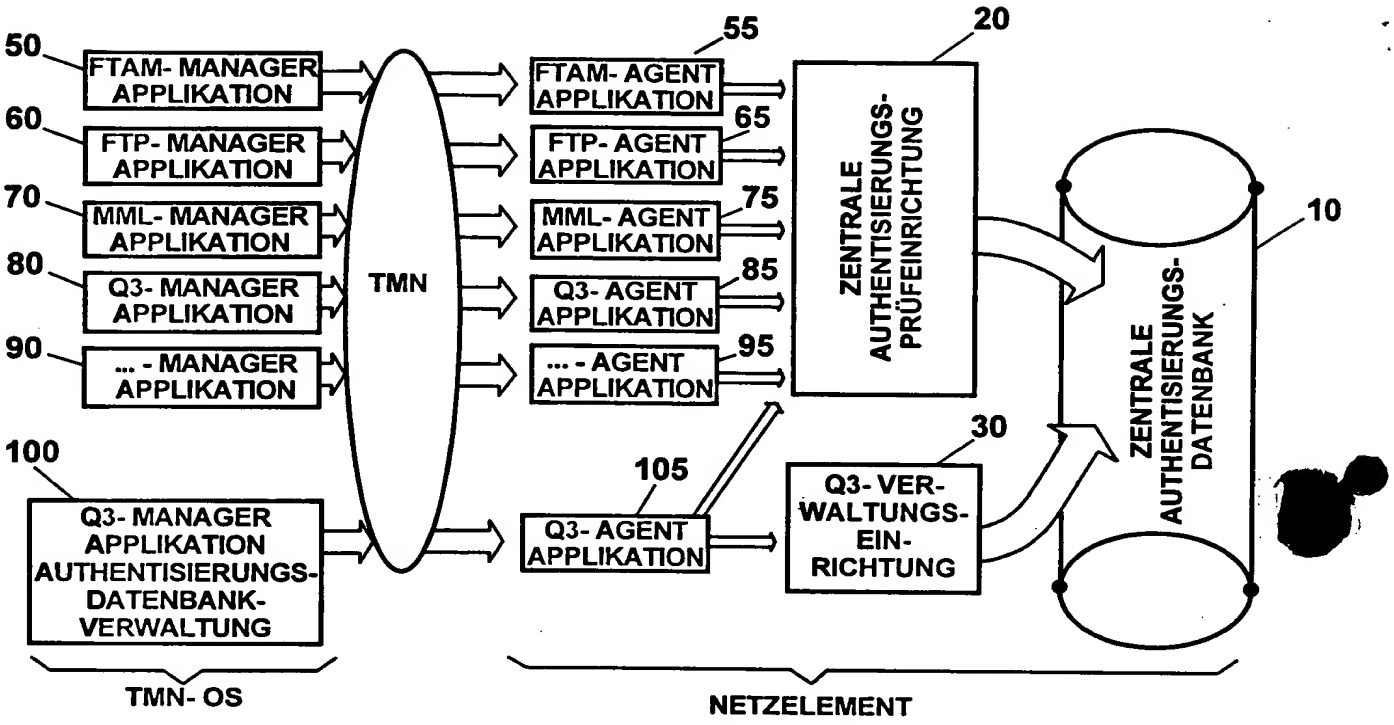

Fig. 1

KOMMUNIKATIONS-PROTOKOLL	INITIATOR	AUTHENTISIERUNGSART
Q3	AET	SIMPLE PASSWORD MECHANISMUS
		REPLAY PROTECTED PASSWORD MECHANISMUS
		NUR IDENTIFIZIERUNG
		CHALLENGE & RESPONSE VERFAHREN
FTAM	USER ID	SIMPLE PASSWORD MECHANISMUS
		REPLAY PROTECTED PASSWORD MECHANISMUS
		CHALLENGE & RESPONSE VERFAHREN
FTP	USER ID	SIMPLE PASSWORD MECHANISMUS
		REPLAY PROTECTED PASSWORD MECHANISMUS
		CHALLENGE & RESPONSE VERFAHREN
MML	USER ID	SIMPLE PASSWORD MECHANISMUS
		REPLAY PROTECTED PASSWORD MECHANISMUS
		CHALLENGE & RESPONSE VERFAHREN

Fig. 2